Rubrik: Markt/Studien

Trotz Fortschritten sind immer noch zwei von drei Systemen anfällig für Exploits

Untersuchung zu den "Gesetzen der Schwachstellen"

(01.12.05) - Gerhard Eschelbeck, CTO und VP Engineering bei Qualys stellte die diesjährigen Ergebnisse seiner Untersuchungen zu den "Gesetzen der Schwachstellen" vor. Die "Gesetze der Schwachstellen" zeigen die neuesten Entwicklungen im Bereich Netzwerk-Sicherheitslücken auf. Die jährlich veröffentlichten Untersuchungen offenbaren neue Entwicklungen im Bereich Sicher-heitslücken und beziehen jetzt auch drahtlose Systeme mit ein. Die aktuelle Studie sieht zwar im vergangenen Jahr erhebliche Verbesserungen beim Patch-Management, belegt aber gleichzeitig, dass immer noch zwei von drei Systemen (also fast 70 Prozent) anfällig sind und potenziell ausgenützt oder angegriffen werden können.

Seit mehr als drei Jahren wertet Eschelbeck statistische Daten über Sicherheitslücken aus, um daraus die "Gesetze der Schwachstellen" abzuleiten. Diese Gesetze machen die aktuellen Entwicklungen auf dem Gebiet der Netzwerksicherheit deutlich und geben so den Unternehmen die Möglichkeit, neue Bedrohungen zu erkennen und ihre eigenen Sicherheitsmaßnahmen mit denen anderer Firmen zu vergleichen. In diesem Jahr basieren die "Gesetze der Schwachstellen" auf der statistischen Analyse von fast 21 Millionen kritischen Schwachstellen, die bei 32 Millionen Live-Netzwerk-Scans entdeckt worden waren. Dies ist die größte derzeit existierende Datenbank für reale Schwachstellen in Netzwerken.

Die Daten zeigen, dass die Unternehmen ihre Patching-Prozesse für interne Systeme um 23 Pro-zent und für externe Systeme um 10 Prozent verbessert haben. Andererseits verkürzt sich jedoch die Zeit von der Bekanntgabe einer Schwachstelle bis zu deren Ausnützung ("Time to Exploit") bei automatisierten Angriffen weiterhin dramatisch. Heute richten automatisierte Angriffe 85 Prozent des von ihnen verursachten Schadens innerhalb der ersten 15 Tage nach ihrem Ausbruch an.

Wie aus der Untersuchung weiter hervorgeht, ist die Bedrohung für drahtlose Systeme derzeit statistisch gesehen sehr gering: Nur eine von fast 20.000 kritischen Sicherheitslücken betraf ein Wireless-Gerät. Jedoch ist eine massive Verlagerung von serverseitigen hin zu clientseitigen Schwachstellen zu beobachten. Mehr als 60 Prozent aller neuen kritischen Schwachstellen sind in Client-Anwendungen zu finden. Bei clientseitigen Schwachstellen muss ein Anwender tätig werden, um die Ausnützung zu ermöglichen - indem er beispielsweise eine bösartige Website aufsucht oder einen infizierten Mail-Anhang öffnet.

"2005 war das Jahr der Verbesserungen beim Patching und Aktualisieren anfälliger Systeme", erklärte Gerhard Eschelbeck, CTO und VP of Engineering bei Qualys. "Das liegt zum großen Teil daran, dass Anbieter wie etwa Microsoft jetzt regelmäßig Advisories mit Patch-Updates heraus-geben - was wiederum dazu führt, dass Unternehmen Sicherheitslücken schneller priorisieren und beseitigen."

Nachstehend eine kurze Zusammenfassung der Ergebnisse:

- **Halbwertszeit:** Die Halbwertszeit beschreibt, wie lange Anwender brauchen, um die Hälfte ihrer Systeme durch Patches zu schützen und so das "Fenster der Gefährdung" zu verkleinern. Im letzten Jahr verkürzte sich die Halbwertszeit kritischer Schwachstellen in externen Systemen von 21 auf 19 Tage und in internen Systemen von 62 auf 48 Tage. Wenn neue Schwachstellen regelmäßig, nach einem vorgegebenen Zeitplan bekannt gemacht werden, installieren Unternehmen die entsprechenden Patches um 18 Prozent schneller.
- **Verbreitung:** Jedes Jahr werden 50 Prozent der am meisten verbreiteten und kritischsten Schwachstellen durch neue Schwachstellen abgelöst.
- **Wirkungsdauer:** Vier Prozent aller kritischen Schwachstellen bleiben bestehen und haben eine unbegrenzte Lebensdauer.
- **Fokus:** 90 Prozent aller Gefährdungen durch Schwachstellen gehen von 10 Prozent der kritischen Schwachstellen aus.
- **Fenster der Gefährdung:** Der Time-to-Exploit-Zyklus schrumpft schneller als der Zyklus der Schwachstellenbeseitigung. 80 Prozent aller Exploits werden innerhalb der ersten Halbwertszeit kritischer Schwachstellen entwickelt.
- **Ausnützung:** Automatisierte Angriffe richten 85 Prozent des von ihnen verursachten Schadens innerhalb der ersten 15 Tage nach ihrem Ausbruch an und haben eine unbegrenzte Lebenszeit.

"Die Untersuchungen zu den "Gesetzen der Schwachstellen" geben Sicherheitsverantwortlichen und Unternehmensleitungen eindeutige, statistisch belegte Informationen an die Hand, auf deren Basis sie fundiertere Entscheidungen treffen können", erklärte Howard A. Schmidt, ehemaliger Berater des Weißen Hauses für Cyber-Sicherheit. "Wenn automatisierte Angriffe 85 Prozent des Gesamtschadens innerhalb der ersten 15 Tage nach ihrem Ausbruch anrichten, so wird es noch entscheidender, dass Unternehmen Bedrohungen schnell erkennen und beseitigen. Die "Gesetze der Schwachstellen" helfen Unternehmen zu verstehen, wie anfällig ihre Systeme wirklich sind und wo sie Prioritäten setzen sollten." (Qualys: ra)